



CVE-2006-4574

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2006-4574
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-10-28 00:07:00 UTC
Updated	2018-10-17 21:38:00 UTC
Description	Off-by-one error in the MIME Multipart dissector in Wireshark (formerly Ethereal) 0.10.1 through 0.99.3 allows remote attack

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	0.10	All	All	All
Application	Wireshark	Wireshark	0.10.13	All	All	All
Application	Wireshark	Wireshark	0.10.4	All	All	All
Application	Wireshark	Wireshark	0.7.9	All	All	All
Application	Wireshark	Wireshark	0.8.16	All	All	All
Application	Wireshark	Wireshark	0.9.10	All	All	All
Application	Wireshark	Wireshark	0.99	All	All	All
Application	Wireshark	Wireshark	0.99.1	All	All	All
Application	Wireshark	Wireshark	0.99.2	All	All	All
Application	Wireshark	Wireshark	0.99.3	All	All	All
Application	Wireshark	Wireshark	0.10	All	All	All
Application	Wireshark	Wireshark	0.10.13	All	All	All
Application	Wireshark	Wireshark	0.10.4	All	All	All
Application	Wireshark	Wireshark	0.7.9	All	All	All
Application	Wireshark	Wireshark	0.8.16	All	All	All
Application	Wireshark	Wireshark	0.9.10	All	All	All
Application	Wireshark	Wireshark	0.99	All	All	All

Application	Wireshark	Wireshark	0.99.1	All	All	All
Application	Wireshark	Wireshark	0.99.2	All	All	All
Application	Wireshark	Wireshark	0.99.3	All	All	All

References

Reference
ASA-2006-255 (RHSA-2006-0726)
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia
Repository / Oval Repository
Advisories - Mandriva Linux
Red Hat update for wireshark - Advisories - Secunia
SecurityFocus
Support
Wireshark Multiple Protocol Dissectors Denial of Service Vulnerabilities
Debian update for ethereal - Advisories - Secunia
Wireshark: wnpa-sec-2006-03
Webmail - OVH
SecurityTracker.com Archives - Wireshark (Ethereal) Bugs in HTTP, LDAP, XOT, WBXML, and MIME Multipart Dissectors Let Remote Users
rPath update for tshark and wireshark - Advisories - Secunia
IBM X-Force Exchange
Security Announcement
issues.rpath.com/browse/RPL-746
Wireshark Multiple Denial of Service Vulnerabilities - Advisories - Secunia
SUSE update for wireshark - Advisories - Secunia
Avaya Products Wireshark Multiple Vulnerabilities - Advisories - Secunia
Debian -- Security Information -- DSA-1201-1 ethereal
20061101-01-P
Mandriva update for wireshark - Advisories - Secunia
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)